Sanitized Copy Approved for Release 2010/11/17 : CIA-RDP87T00623R000200070011-7

Director of Central Intelligence
Security Committee
Computer Security Subcommittee

10 January 1985
DCISEC-CSS-M169

1. The one hundred and sixty-ninth session of the Computer Security Subcommittee was convened on 19 December 1984 at the
STAT [redacted] in McLean, VA. In attendance were:

STAT [redacted] Chairman
STAT [redacted] Executive Secretary
Mr. James Schenken, U.S. Secret Service
STAT [redacted] CIA
Mrs. Martha Tofferi, Air Force
STAT [redacted] NSA
Major Jack Freeman, Army
Ms. Karen Deneroff, Depart of State
STAT [redacted] SECOM
Mr. Gene Epperly, OSD

2. The opening discussions concerned a proposed SECOM allocation of $70K for FY85. Suggestions for areas of study to be supported were:

- information collection (i.e. Navy efforts reported in previous minutes)

- tamper detection methods

- enhanced user authentication (e.g. IBM signature identifier)

- testing/assessment of security products

- guidance on standards/guidelines for personal computers

- computer security education (e.g. DoDCI).

The subcommittee's preferences appeared to be primarily in the areas of collection requirements, education, and PC usage guidelines. The Chairman requested the State member to contact NBS (Steinauer) to determine their ability and willingness to draft a strawman guideline for the usage of personal computers in a secure environment. He stated that his specific concern was in the area of connection of PC's into local area networks (LAN's). Accordingly, he also requested the CIA member to arrange a presentation to the Subcommittee by CIA's R&D organization on their concepts for LAN architecture for their new facilities.

Sanitized Copy Approved for Release 2010/11/17 : CIA-RDP87T00623R000200070011-7

Sanitized Copy Approved for Release 2010/11/17 : CIA-RDP87T00623R000200070011-7

3. The Executive Secretary announced to the membership that the DoD Computer Security Center had recently completed the technical aspects of the evaluation of the Honeywell SCOMP. He reported that the team's findings and conclusions were successfully defended before an internal senior technical review board, and that the Center was preparing to officially inform Honeywell that the SCOMP has achieved an A1 rating (as defined in the DoD Trusted Computer System Evaluation Criteria).

4. The Chairman discussed the need for an annual report, and volunteered to prepare a draft.

5. Mr. Epperly reported on the first meeting of the Automated Information System Security Subcommittee (AISS) of the National Telecommunications and Information System Security Committee (NTISSC). Among the deliberations of the AISS was the question of the authority of the NTISSC vis-a-vis the DCI authority/responsibility for computer security within the Intel Community. He reported that it was suggested that the DCI is still responsible for issuing policy and guidance for the protection of foreign intelligence and SCI. This was seen as a clear thrust to begin to further define the various roles and responsibilities delineated in NSDD-145.

6. The next subject was the re-write of DCID 1/16. At the previous meeting, it was suggested that we re-examine the current draft in light of recent developments such as the acceptance of the DoDCSC's Evaluation Criteria, and the current efforts to develop implementation guidelines (i.e., the Environments Document). The Chairman asked for viewpoints as to what, if any, adjustments should be considered to the latest draft of the DCID. In short, the sense of the Subcommittee was that the DCID should retain the basic structure and thrust of the latest draft, but be made consistent with the Criteria and the Environments Document. Other major points made were that the DCID retain its sensitivity to system functionality, and that the revised document be non-traumatic to current systems. That is, that there be no radical departures for existing policy.

STAT

[redacted]

Executive Secretary

Sanitized Copy Approved for Release 2010/11/17 : CIA-RDP87T00623R000200070011-7